

# LDPC codes from Singer cycles

Luca Giuzzi

Angelo Sonnino

Dipartimento di Matematica  
Politecnico di Bari  
Via Orabona, 4  
70125 Bari, Italy  
*Email:* giuzzi@poliba.it

Dipartimento di Matematica e Informatica  
Università della Basilicata  
Campus Macchia Romana  
Viale dell'Ateneo Lucano, 10  
85100 Potenza, Italy  
*Email:* angelo.sonnino@unibas.it

1st February 2008

## Abstract

The main goal of coding theory is to devise efficient systems to exploit the full capacity of a communication channel, thus achieving an arbitrarily small error probability. Low Density Parity Check (LDPC) codes are a family of block codes—characterised by admitting a sparse parity check matrix—with good correction capabilities. In the present paper the orbits of subspaces of a finite projective space under the action of a Singer cycle are investigated.

## 1 Introduction

A  $[n, k, d]$ -linear code over  $\text{GF}(q)$  is a monomorphism  $\theta$  from  $M = \text{GF}(q)^k$  into  $R = \text{GF}(q)^n$  such that the images of any two distinct vectors  $\mathbf{m}_1, \mathbf{m}_2 \in M$  differ in at least  $d$  positions. The elements of  $M$  are called messages, while the elements of the image  $\mathcal{C} = \theta(M)$  are the codewords of  $\theta$ . The function

$$d : \begin{cases} R \times R \mapsto \mathbb{N} \\ (\mathbf{x}, \mathbf{y}) \mapsto |\{i : x_i - y_i \neq 0\}| \end{cases}$$

is the *Hamming distance on  $R$* . In the present paper we shall usually identify a code with the set of its codewords.

The problem of *minimum distance decoding* is to find, for any given vector  $\mathbf{r} \in R$  the set  $\mathcal{C}_{\mathbf{r}}$  of all the codewords  $\mathbf{c} \in \mathcal{C}$  at minimum Hamming distance from  $\mathbf{r}$ . If  $\mathcal{C}_{\mathbf{r}}$  contains just one element  $\mathbf{c}$ , then we can uniquely determine a message  $\mathbf{m}$  such that  $\theta(\mathbf{m}) = \mathbf{c}$  and we state that the decoding of  $\mathbf{r}$  has succeeded; otherwise, we remark that it has not been possible to correctly recover the message originally sent.

Minimum distance decoding is, in general, a hard problem, see [2]; in fact, many algorithms currently in use sacrifice some of the abstract correcting capabilities of a code in favour of ease of implementation and lower complexity; notable examples are the syndrome decoding technique for general linear codes and the Welch–Berlekamp approach for BCH codes, see [17]. We remark, however, that even these techniques may be prohibitively expensive when the length  $n$  of the code, that is the dimension of the vector space  $R$ , is large.

On the other hand, long codes present several advantages, since it can be shown that almost all codes with large  $n$  have excellent correction capabilities, see [16]. It is thus important to find some special families of codes for which good encoding and decoding techniques are known.

Low Density Parity Check (LDPC) codes have been introduced by Gallager in [10],[9] and then, ignored for almost 30 years. They have been recently rediscovered, see [15]; and it has been realised that they may be applied to high-speed, high-bandwidth digital channels and support efficient decoding algorithms based upon message-passing strategies. Furthermore, the performance of some of these codes is remarkably close to the Shannon limit for the AWGN channel; consequently, they turn out to be very competitive, even when compared with more elaborate constructions, like turbo codes, see [15]. Nevertheless, the problem of providing efficient encoding is, in general, non-trivial, see [5], although, in several cases, manageable, see [18]. This motivates the search for new ways of constructing suitable parity-check matrices for broad classes of LDPC codes.

A linear code is Low Density Parity Check (for short, LDPC) if it admits at least one sparse parity check matrix. In particular, a LDPC code is *regular* if the set of its codewords is the null space of a parity check matrix  $\mathbf{H}$  with the following structural properties:

- (L1) each row of  $\mathbf{H}$  contains  $k$  non-zero entries;
- (L2) each column of  $\mathbf{H}$  contains  $r$  non-zero entries;
- (L3) the number of non-zero entries in common between any two distinct columns of  $\mathbf{H}$  is at most 1;
- (L4) both  $k$  and  $r$  are small compared with the length  $n$  of the code and the number of rows in  $\mathbf{H}$ .

In this paper we describe an algorithm for the construction of such parity-check matrices based on the orbits of subspaces of a finite projective space  $\text{PG}(n-1, q)$ , with  $q$  even, under the action of a Singer cycle. More precisely, some cyclic and almost cyclic LDPC codes are constructed using some suitable representatives for each of these orbits.

## 2 Preliminaries: incidence matrices

There is a straightforward correspondence between finite incidence structures and binary matrices. This topic has been widely investigated, also in the context of coding theory; see [1].

Given a binary matrix  $M$ , it is always possible to introduce an incidence structure  $\mathcal{S}_M = (\mathcal{P}, \mathcal{L}, I)$  such that the points  $\mathcal{P}$  are the columns of  $M$ , the blocks  $\mathcal{L}$  are the rows of  $M$  and  $P \in \mathcal{P}$  is incident with  $L \in \mathcal{L}$  if and only if  $m_{LP} = 1$ . Conversely, given an incidence structure  $\mathcal{S}$  with point-set  $\mathcal{P} = \{p_1, p_2, \dots, p_v\}$  and block-set  $\mathcal{L} = \{l_1, l_2, \dots, l_b\}$ , the *incidence matrix*  $M = (m_{ij})$  of  $\mathcal{S}$  is the binary  $b \times v$ -matrix with

$$m_{ij} = \begin{cases} 1 & \text{if } p_j I l_i \\ 0 & \text{otherwise.} \end{cases}$$

Recall that an incidence structure  $\mathcal{S} = (\mathcal{P}, \mathcal{L}, I)$  is written simply as  $(\mathcal{P}, \mathcal{L})$  when any element  $L \in \mathcal{L}$  is a subset of  $\mathcal{P}$ , and given  $p \in \mathcal{P}$  and  $L \in \mathcal{L}$ , we have  $pIL$  if, and only if,  $p \in L$ .

A map  $\varphi : \mathcal{P} \cup \mathcal{L} \rightarrow \mathcal{P} \cup \mathcal{L}$  is a collineation of  $\mathcal{S}$  when  $\varphi$  maps points into points, blocks into blocks and preserves all incidences.

In particular, we are interested in incidence structures endowed with collineation group  $G$  acting regularly on the points. In this case it is quite easy to write all the blocks in  $\mathcal{L}$  and the associated incidence matrix  $\mathbf{H}$  has a special form. We proceed as follows.

Fix a point  $P \in \mathcal{P}$  and let  $\mathcal{T} = \{\ell_1, \ell_2, \dots, \ell_h\}$  be the set of all blocks of  $\mathcal{S}$  incident with  $P$  and such that:

1.  $\ell_i^g \neq \ell_j$  for any  $g \in G$  and  $1 \leq i < j \leq h$ ;
2. for any line  $\ell \in \mathcal{L}$  there is a block  $\ell_i \in \mathcal{T}$  and a  $g \in G$  such that  $\ell = \ell_i^g$ .

The set  $\mathcal{T}$  is called a *starter set* for  $\mathcal{S}$ , see [6]. Clearly,

$$\bigcup_{j=1}^h \{\ell_j^g \mid g \in G\};$$

therefore, the whole incidence matrix  $\mathbf{H}$  of  $\mathcal{S}$  can be reconstructed by just providing a suitable starter set  $\mathcal{T}$  and generators of the group  $G$ .

If we further suppose  $G$  to be cyclic, let  $\tau$  be one of its generators, then the incidence structure

$$\mathcal{S} = (\mathcal{P}, \{\ell_j^{\tau^i} \mid 1 \leq i \leq |G|, 1 \leq j \leq h\})$$

admits at least a circulant incidence matrix  $\mathbf{H}$ ; that is, a block matrix  $\mathbf{H}$  of type

$$\mathbf{H} = \begin{pmatrix} H_1 \\ \vdots \\ H_h \end{pmatrix}$$

wherein any row  $H_j$ ,  $j > 1$  is obtained from the preceding one  $H_{j-1}$  by applying a cyclic right shift. Clearly, this happens provided that the points and blocks of  $\mathcal{S}$  are arranged in such a way as  $P_i = P^{i-1}$  and  $\ell_i = \ell_j^{\tau^{i-1}}$  with  $j \in \{1, 2, \dots, h\}$ .

### 3 Preliminaries: projective spaces and spreads

Let  $\text{PG}(V, \mathbb{F})$  be the projective space whose elements are the vector subspaces of the vector space  $V$  over the field  $\mathbb{F}$ . We denote by the same symbol a 1-dimensional vector subspace of  $V$  and the corresponding element of  $\text{PG}(V, \mathbb{F})$ . An element  $T$  of  $\text{PG}(V, \mathbb{F})$  has *rank*  $t$  and *dimension*  $t - 1$ , whenever  $T$  has dimension  $t$  as a vector space over  $\mathbb{F}$ . When the dimension of  $V$  over  $\mathbb{F} = \text{GF}(q)$  is finite and equal to  $n$ , we shall usually write  $\text{PG}(n - 1, q)$  instead of  $\text{PG}(V, \mathbb{F})$ . The elements of rank 1, 2, 3 and  $n - 1$  in  $\text{PG}(n - 1, q)$  are called respectively *points*, *lines*, *planes* and *hyperplanes*. Points contained in the same line are said to be *collinear*. Observe that, for any  $i \geq 1$ ,

$$\text{PG}_i(V) = (\mathcal{P}, \mathcal{L}),$$

where  $\mathcal{P} = \{W \leq V : \dim W = 1\}$  and  $\mathcal{L} = \{X \leq V : \dim X = i + 1\}$  is an incidence structure.

Let now  $\{E_0, E_1, \dots, E_{n-1}\}$  be a fixed basis of  $V$ . Then, we say that the point  $\langle x_0 E_0 + x_1 E_1 + \dots + x_{n-1} E_{n-1} \rangle$  of  $\text{PG}(V, \mathbb{F})$  has homogeneous projective coordinates  $(x_0, x_1, \dots, x_{n-1})$ .

The number of points of  $\text{PG}(n - 1, q)$  is

$$\frac{q^n - 1}{q - 1} = q^{n-1} + \dots + q + 1,$$

while the number of its lines is

$$\frac{(q^n - 1)(q^{n-1} - 1)}{(q^2 - 1)(q - 1)},$$

see [12]. In particular, the number of lines of  $\text{PG}(2, q)$ ,  $\text{PG}(3, q)$  and  $\text{PG}(4, q)$  are respectively  $q^2 + q + 1$ ,  $(q^2 + 1)(q^2 + q + 1)$  and  $(q^2 + 1)(q^4 + q^3 + q^2 + q + 1)$ .

The points and the lines of a projective space  $\text{PG}(n - 1, q)$  form a 2-design, whose incidence matrix  $M$  defines a regular LDPC code, called  $\mathbb{PG}^{(1)}$  in [13]. The code defined by the transposed matrix  $M$  is also LDPC and it is called  $\mathbb{PG}^{(2)}$  in the aforementioned paper.

An application  $A$  of  $V$  in itself is a semilinear map if, and only if, there is an automorphism  $\mu$  of  $\mathbb{F}$  such that for all vectors  $v, w \in V$  and all elements  $\alpha \in \mathbb{F}$ ,

$$(v + w)^A = v^A + w^A, \quad (\alpha v)^A = \alpha^\mu v^A.$$

If  $A$  is a bijection, then we say that it is *non-singular*. When  $\mu = \text{id}$ , then  $A$  is called *linear*. Any non-singular semilinear map of  $V$  in itself induces a collineation  $\tau_A$  of  $\text{PG}(V, \mathbb{F})$  which maps the point  $\langle v \rangle$  into the point  $\langle v^A \rangle$ . Conversely, given any collineation  $\tau$  of  $\text{PG}(V, \mathbb{F})$ , there is a non-singular semilinear map  $A$  of  $V$  such that  $\tau = \tau_A$ .

A Singer cycle  $S$  is a cyclic collineation group of  $\text{PG}(n - 1, q)$  acting regularly on the points; that is to say that  $S$  has order  $q^{n-1} + \dots + q + 1$ , is cyclic and only the

identity fixes any point. If  $S$  and  $S'$  are two Singer cycles of  $\text{PG}(n-1, q)$ , then there is a collineation  $\tau$  of  $\text{PG}(n-1, q)$  such that  $S' = \tau^{-1}S\tau$ .

As usual, we write  $\text{PG}(n-1, q)$  for  $\text{PG}(\text{GF}(q^n), \text{GF}(q))$ . Let  $\alpha$  be a generator of the multiplicative group of  $\text{GF}(q^n)$ ; then, the map  $\sigma$  of  $\text{GF}(q^n)$  into itself defined by  $\sigma : x \mapsto \alpha x$  is a non-singular  $\text{GF}(q)$ -linear map. Observe that  $\sigma$ , as a linear map, has order  $q^n - 1$  and defines a collineation of  $\text{PG}(n-1, q)$  of order  $q^{n-1} + \dots + q + 1$  acting transitively on the points of  $\text{PG}(n-1, q)$ ; hence, the collineation group  $S$  generated by  $\sigma$  is indeed a Singer cycle of  $\text{PG}(n-1, q)$ .

We can regard the projective space  $\text{PG}(n-1, q) = \text{PG}(V, \text{GF}(q))$  as a distinguished hyperplane of  $\text{PG}(n, q) = \text{PG}(V', \text{GF}(q))$ , with  $V' = \langle E \rangle \oplus V$ . Let now  $\sigma$  be the generator of a Singer cycle of  $\text{PG}(n-1, q)$ . The map

$$\sigma' : xE + v \mapsto xE + v^\sigma$$

gives a cyclic collineation group  $\tilde{S}$  of order  $q^n - 1$ , which induces a Singer cycle on the hyperplane  $\text{PG}(n-1, q)$  and acts regularly on the points of  $\text{PG}(n, q) \setminus \text{PG}(n-1, q)$  different from  $\langle E \rangle$ . Furthermore, this group  $\tilde{S}$  acts transitively on the lines of  $\text{PG}(n, q)$  incident with  $\langle E \rangle$ .

A  $(t-1)$ -spread  $\mathcal{S}$  of a projective space  $\text{PG}(n-1, q)$  is a family of mutually disjoint subspaces, each of rank  $t$ , such that each point of  $\text{PG}(n-1, q)$  belongs to exactly one element of  $\mathcal{S}$ . It has been proved by Segre [19] that a  $(t-1)$ -spread of  $\text{PG}(n-1, q)$  exists if and only if  $n = rt$ . A spread  $\mathcal{S}$  with  $t = 2$  is called *line-spread*.

Let now  $\mathcal{S}$  be a  $(t-1)$ -spread of  $\text{PG}(rt-1, q)$ . It is possible to embed  $\text{PG}(rt-1, q)$  into  $\text{PG}(rt, q)$  as a hyperplane, and then to introduce a new incidence structure  $A(\mathcal{S})$  as follows. The points of  $A(\mathcal{S})$  are the points of  $\text{PG}(rt, q) \setminus \text{PG}(rt-1, q)$ . The lines of  $A(\mathcal{S})$  are the  $t$ -dimensional subspaces of  $\text{PG}(rt, q)$  which are not contained in  $\text{PG}(rt-1, q)$  but contain an element of  $\mathcal{S}$ . The incidence relation is the natural set-theoretical one. The incidence structure  $A(\mathcal{S})$  is a  $2 - (q^{rt}, q^t, 1)$  translation design with parallelism, see [3]. The  $(t-1)$ -spread  $\mathcal{S}$  is called Desarguesian when  $A(\mathcal{S})$  is isomorphic to the affine space  $AG(r, q^t)$ . We provide two different characterisations of Desarguesian spreads, according as  $r = 2$  or  $r \neq 2$ .

When  $r = 2$ , the projective space has dimension  $2t-1$ . A *regulus*  $\mathcal{R}$  of  $\text{PG}(2t-1, q)$  is a set of  $q+1$  mutually disjoint  $(t-1)$ -dimensional subspaces such that each line intersecting three elements of  $\mathcal{R}$  has a point in common with all the subspaces of  $\mathcal{R}$ .

If  $A, B, C$  are three mutually disjoint  $(t-1)$ -dimensional subspaces of  $\text{PG}(2t-1, q)$ , then there is a unique regulus  $\mathcal{R}(A, B, C)$  of  $\text{PG}(2t-1, q)$  containing  $A, B$  and  $C$ . A spread  $\mathcal{S}$  is *regular* if the regulus  $\mathcal{R}(A, B, C)$  is contained in  $\mathcal{S}$  whenever  $A, B$  and  $C$  are three distinct element of  $\mathcal{S}$ .

**Theorem 1** ([8]). *Suppose  $q > 2$ . A  $(t-1)$ -spread  $\mathcal{S}$  of  $\text{PG}(2t-1, q)$  is Desarguesian if and only if it is regular.*

We now consider the case  $r > 2$ . A  $(t-1)$ -spread is *normal* when it induces a spread in any subspace generated by any two of its elements, see [14]. In particular, fix  $T = \langle A, B \rangle$  with  $A, B \in \mathcal{S}$ . Then, for any  $C \in \mathcal{S}$ , either  $C \subseteq T$  or  $C \cap \mathcal{S} = \emptyset$ . Such spreads are called *geometric* in [19].

**Theorem 2** ([3]). *For  $r > 2$ , the  $(t-1)$ -spread  $\mathcal{S}$  is Desarguesian if and only if it is normal.*

## 4 The $\text{GF}(q)$ -linear representation of $\text{PG}(r-1, q^t)$

Let  $V$  be a  $r$ -dimensional vector space over  $\text{GF}(q^t)$ , and let, as usual,  $\text{PG}(r-1, q^t) = \text{PG}(V, \text{GF}(q^t))$ .

We may regard  $V$  as a vector space of dimension  $rt$  over  $\text{GF}(q)$ ; hence, each point  $\langle x \rangle$  of  $\text{PG}(r-1, q^t)$  determines a  $(t-1)$ -dimensional subspace  $P(x)$  of the projective space  $\text{PG}(V, \text{GF}(q)) = \text{PG}(rt-1, q)$ ; likewise, each line  $l$  of  $\text{PG}(r-1, q^t)$  defines a  $(2t-1)$ -dimensional subspace  $P(l)$  of  $\text{PG}(rt-1, q)$ .

Write  $\mathcal{L}$  for the set of all  $(t-1)$ -dimensional subspaces of  $\text{PG}(V, \text{GF}(q))$ , each obtained as  $P(x)$ , with  $x$  a point of  $\text{PG}(r-1, q^t)$ . Then,  $\mathcal{L}$  is a  $(t-1)$ -spread of  $\text{PG}(rt-1, q)$ ; this is called the  $\text{GF}(q)$ -linear representation of  $\text{PG}(r-1, q^t)$ . It has been shown that  $\mathcal{L}$  is Desarguesian and any Desarguesian spread of  $\text{PG}(rt-1, q)$  is isomorphic to  $\mathcal{L}$ , see [8] for  $r = 2$  and [19], [3] for  $r > 2$ .

**Theorem 3.** *A  $(t-1)$ -spread  $\mathcal{S}$  of  $\text{PG}(rt-1, q)$  is Desarguesian if and only if there is a collineation group of  $\text{PG}(rt-1, q)$  of order  $q^{t-1} + q^{t-2} + \dots + q + 1$  fixing all elements of  $\mathcal{S}$ .*

*Proof.* Denote by  $T$  the translation group of  $A(\mathcal{S})$ , that is, the group of all elations of  $\text{PG}(rt, q)$  with axis  $\text{PG}(rt-1, q)$ . Let  $O$  be a fixed point of  $A(\mathcal{S})$ . For each line  $L$  of  $A(\mathcal{S})$  incident with  $O$ , denote by  $T_L$  the stabiliser of  $L$  in  $T$ ; take also  $\mathcal{K}$  to be the family of all the subgroups  $T_L$  of  $T$ . We know that  $T$  is elementary abelian and  $T_L$  is transitive on the points of the line  $L$ . We may now introduce a new incidence structure  $\pi$ , whose points are the elements of  $T$  and whose lines are the lateral classes of the subgroups  $T_L$ . Given a point  $P \in A(\mathcal{S})$ , denote by  $\tau_{O,P}$  the element of  $T$  which maps  $O$  into  $P$ . The map  $P \mapsto \tau_{O,P}$  turns out to be an isomorphism between  $A(\mathcal{S})$  and  $\pi$ .

The *kernel*  $K$  of  $\mathcal{K}$  is the set of all the endomorphisms  $\alpha$  of  $T$  such that  $T_L^\alpha \subset T_L$ . It has been shown in [7] that  $K$  is a field. Hence,  $T$  is a vector space over  $K$  and each element of  $\mathcal{K}$  is a vector subspace of  $T$ . Given any central collineation  $\omega$  of  $\text{PG}(rt, q)$  with axis  $\text{PG}(rt-1, q)$  and centre  $O$ , the map  $\bar{\omega}$  of  $T$  into itself defined by  $\bar{\omega} : \tau \mapsto \omega\tau\omega$  is an element of  $K$ . Hence,  $K$  contains a subfield isomorphic to  $\mathbb{F} = \text{GF}(q)$ .

Let now  $E$  be a subfield of  $K$  and denote by  $\text{PG}(T, E)$  the projective space associated to  $T$ , regarded as a vector space over  $E$ , and by  $\mathcal{K}(E)$  the spread of  $\text{PG}(T, E)$  induced by  $\mathcal{K}$ . The designs  $\pi$  and  $A(\mathcal{K}(E))$  are isomorphic. Furthermore, the  $(t-1)$ -spreads  $\mathcal{S}$  and  $\mathcal{K}(F)$  are also isomorphic, that is, there is a collineation  $\tau$  of  $\text{PG}(rt-1, q)$  such that  $\mathcal{S}^\tau = \mathcal{K}(F)$ , see [7].

It follows that the spread  $\mathcal{S}$  is Desarguesian if and only if  $T_L$  has dimension 1 over  $K$ , see [7]. This condition is equivalent to require that  $K$  has order  $q^t - 1$  and defines a collineation group of  $\text{PG}(rt-1, q)$  of order  $q^{t-1} + q^{t-2} + \dots + q + 1$  fixing all the elements of  $\mathcal{K}(F)$ .  $\square$

**Theorem 4.** *Let  $S$  be a Singer cycle of  $\text{PG}(n-1, q)$ , with  $n = rt$ . Denote by  $S_1$  and  $S_2$  respectively the subgroups of  $S$  of order  $\frac{q^t-1}{q-1}$  and  $\frac{q^n-1}{q^t-1}$ , so that  $S = S_1 \times S_2$ . Then, there is a Desarguesian  $(t-1)$ -spread  $\mathcal{S}$  of  $\text{PG}(n-1, q)$  such that  $S_2$  acts regularly on  $\mathcal{S}$  and  $S_1$  fixes all its elements.*

*Proof.* Write  $\text{PG}(n-1, q) = \text{PG}(\text{GF}(q^n), \text{GF}(q))$  and assume  $S$  to be the Singer cycle spanned by the collineation  $\sigma : x \mapsto \alpha x$ , where  $\alpha$  is a generator of the multiplicative group of  $\text{GF}(q^n)$ .

As  $t$  divides  $n$ , the element  $\beta = \alpha^{\frac{q^n-1}{q^t-1}}$  is a generator of the multiplicative group of the subfield  $\text{GF}(q^t)$  of  $\text{GF}(q^n)$ . Now let  $S_1$  be the subgroup of  $S$  generated by  $\sigma_1 = \sigma^{\frac{q^n-1}{q^t-1}}$ . Then,  $\mathcal{S} = \{ \text{GF}(q^t)x \mid x \in \text{GF}(q^n) \}$  is a  $(t-1)$ -spread of  $\text{PG}(n-1, q)$  which is preserved by  $S_1$ . As  $S_1$  acts over each member of  $\mathcal{S}$  as a Singer cycle, by Theorem 3 we conclude that  $\mathcal{S}$  is Desarguesian.

If  $\gamma$  is a primitive element of  $\text{GF}(q^n)$  over  $\text{GF}(q^t)$ , then the collineation defined by the map  $\sigma_2 : x \mapsto \gamma x$  defines a subgroup  $S_2$  of  $S$  of order  $\frac{q^n-1}{q^t-1}$ . By construction,  $S = S_1 \times S_2$ . As  $\mathcal{S} = \{ \text{GF}(q^t)\gamma^j \mid (q^t)^{r-1} + \dots + q^t + 1 \geq j \geq 0 \}$ , the group  $S_2$  preserves the  $(t-1)$ -spread  $\mathcal{S}$  and acts regularly on its elements.  $\square$

## 5 Decomposition of $\text{PG}(n-1, q)$ for $n$ odd

For odd  $n$  any line of  $\text{PG}(n-1, q)$  has an orbit of length  $\frac{q^n-1}{q-1}$  under the action of a Singer cycle  $S$  of the space. Hence, we can decompose the set of all lines of  $\text{PG}(n-1, q)$  into  $\frac{q^{n-1}-1}{q^2-1}$  orbits under the action of  $S$ . Each of these orbits, say  $i$  for  $1 \leq i \leq \frac{q^{n-1}-1}{q^2-1}$ , defines a cyclic structure whose incidence matrix  $M_i$  is circulant. Hence, the incidence matrix  $M$  of  $\mathbb{PG}^{(1)}$  has the following structure:

$$M = \begin{pmatrix} M_1 \\ M_2 \\ \vdots \\ M_{(q^{n-1}-1)/(q^2-1)} \end{pmatrix}.$$

A starter set of  $\text{PG}(n-1, q)$  can be obtained as follows. Let  $\sigma$  be a generator of the Singer cycle  $S$  and choose a point  $P$ . Fix a line  $l$  incident with  $P$ , suppose that  $i_0 = 0, i_1, \dots, i_q$  are integers, and  $P = P^{\sigma^{i_0}}, P_1 = P^{\sigma^{i_1}}, \dots, P_q = P^{\sigma^{i_q}}$  are the points of  $l$ . Then,  $l_j = l^{\sigma^{i_j}}$ ,  $0 \leq j \leq q$  are exactly the  $q+1$  lines of the orbit of  $l$  under the action of  $S$  which are incident with  $l$ . Hence, a starter set of  $\text{PG}(n-1, q)$  is just  $\mathbf{S} = \{s_1, s_2, \dots, s_{\frac{q^{n-1}-1}{q^2-1}}\}$ , consisting of  $\frac{q^{n-1}-1}{q^2-1}$  lines incident with  $P$  such that, if  $P^{\sigma^h}$  belongs to  $s_i$ , then  $s_i^{\sigma^h}$  does not belong to  $\mathbf{S}$ .

## 6 Decomposition of $\text{PG}(n-1, q)$ for $n$ even

Suppose now  $n = 2t$  with  $t > 1$  and denote by  $S$  a Singer cycle of  $\text{PG}(n-1, q)$ .

Write  $S = S_1 \times S_2$ , where  $S_1$  has order  $\frac{q^2-1}{q-1}$  and  $S_2$  has order  $\frac{q^{2t}-1}{q^2+1}$ . By Theorem 4, there is a Desarguesian line spread  $\mathcal{S}$  of  $\text{PG}(2t-1, q)$  such that  $S_1$  fixes all the lines of  $\mathcal{S}$  and  $S_2$  acts regularly its elements.

**Lemma 1.** *The stabiliser in  $S$  of a line  $m$  not in  $\mathcal{S}$  is the identity.*

*Proof.* It has been proved in [20], that there are exactly  $\frac{q^n-1}{q^2-1}$  lines of  $\text{PG}(n-1, q)$  whose stabiliser in  $S$  is different from the identity. Since any line of  $\mathcal{S}$  is fixed by  $S_1$  and  $\mathcal{S}$  contains exactly  $\frac{q^n-1}{q^2-1}$  of them, the stabiliser in  $S$  of a line  $m$  not in  $\mathcal{S}$  is the identity.  $\square$

The set of all the lines of  $\text{PG}(n-1, q)$  can be decomposed into the set  $\mathcal{S}$  and  $q(q^{2t-4} + q^{2t-6} + \dots + q^2 + 1)$  other orbits under the action of  $S$ , each of length  $\frac{q^{2t}-1}{q-1}$ . These orbits, say  $i$ , for  $1 \leq i \leq q(q^{2t-4} + \dots + q^2 + 1)$  define a cyclic structure whose incidence matrix  $M_i$  is circulant. Hence, the incidence matrix  $M$  of  $\mathbb{PG}^{(1)}$  has in this case the following structure

$$M = \begin{pmatrix} M_0 \\ M_1 \\ \vdots \\ M_{q(q^{2t-2}-1)/(q^2-1)} \end{pmatrix},$$

where  $M_0$  is the incidence matrix of the structure induced on  $\mathcal{S}$ . The points of  $\text{PG}(n-1, q)$  may be indexed in such a way as to have

$$M_0 = \begin{pmatrix} B_1 & B_2 & \cdots & B_{q+1} \end{pmatrix},$$

where  $B_1 = B_2 = \dots = B_{q+1}$  is the identity matrix of order  $q^{n-1} + q^{n-2} + \dots + q + 1$ .

## 7 The case of $\text{PG}(3, 2^e)$

In order to investigate the details of what happens in  $\text{PG}(3, 2^e)$  we need to recall some properties of elliptic quadrics and regular spreads in this space. The interested reader might look at [11] for a proof of the results.

Denote by  $Q^-(3, q)$  the set of all points of  $\text{PG}(3, q)$  whose homogeneous coordinates are solution of the equation

$$X_0X_1 + X_2^2 + bX_2X_3 + cX_3^2 = 0,$$

where  $b$  and  $c$  are such that  $\xi^2 + b\xi + c$  is an irreducible polynomial over  $\text{GF}(q)$ .

A set of points  $\mathcal{O}$  is an *elliptic quadric* if there is a collineation  $\tau$  of  $\text{PG}(3, q)$  such that  $\mathcal{O}^\tau = Q^-(3, q)$ . A line, which intersects  $\mathcal{O}$  in exactly one point is called *tangent*. Likewise, a plane which intersects  $\mathcal{O}$  in a exactly one point is also called *tangent*. The following properties are straightforward:

1.  $\mathcal{O}$  contains exactly  $q^2 + 1$  points;
2. no three points of  $\mathcal{O}$  are collinear;



3. a plane meets  $\mathcal{O}$  in either exactly one or in  $q + 1$  points;
4. if  $P$  is a point of  $\mathcal{O}$ , then the lines tangent to  $\mathcal{O}$  at  $P$  are contained in the plane tangent to  $\mathcal{O}$  in  $P$ ;
5. there is a subgroup of order  $q^2 + 1$  of  $\text{PGL}(4, q)$  which acts transitively on  $\mathcal{O}$ .

Let now  $\mathcal{S}$  be a regular spread of  $\text{PG}(3, 2^e)$ . Then, there is an elliptic quadric  $\mathcal{O}$  such that:

1. any line of  $\mathcal{S}$  is tangent to  $\mathcal{O}$ ;
2. the subgroup  $S_2$  of order  $q^2 + 1$  of the Singer cycle  $S$  which stabilises  $\mathcal{S}$ , acts regularly on  $\mathcal{O}$ .

Let  $S_1 = \langle \tau \rangle$  be the subgroup of  $S$  of order  $q + 1$  which fixes all the lines of  $\mathcal{S}$  and acts transitively on the points of any line of the spread. Then,  $\mathcal{O}_i = \mathcal{O}^{\tau^i}$ , for  $i = 0, 1, \dots, q$  is an elliptic quadric and any line of  $\mathcal{S}$  is tangent to  $\mathcal{O}_i$ ; indeed,  $\{\mathcal{O}_0, \mathcal{O}_1, \dots, \mathcal{O}_q\}$  is a partition of point-set of  $\text{PG}(3, q)$ .

**Lemma 2.** *For any line  $l$  of  $\text{PG}(3, q)$  not in  $\mathcal{S}$  there is a unique quadric  $\mathcal{O}_i$  such that  $l$  is tangent to  $\mathcal{O}_i$ .*

*Proof.* As  $q$  is even, there is a symplectic polarity  $\perp$  of  $\text{PG}(3, q)$  such that a line is totally isotropic with respect to  $\perp$  if and only if it is tangent to  $\mathcal{O}$ .

Call  $\pi$  the symplectic polarity induced by  $\mathcal{O}_i$  for  $i \neq 0$ . Then, a line of  $\text{PG}(3, q)$  is totally isotropic simultaneously respect to  $\perp$  and to  $\pi$  if and only if  $l$  belongs to  $\mathcal{S}$ , see[11]. Hence, no line is tangent to both  $\mathcal{O}$  and  $\mathcal{O}_i$ . Thus,  $\mathcal{O}_i$  and  $\mathcal{O}_j$  do not have any common tangent for  $i \neq j$ .

Any elliptic quadric  $\mathcal{O}_i$  has  $(q^2 + 1)(q + 1)$  tangent lines; as  $q^2 + 1$  of these belong to  $\mathcal{S}$ , we obtain that there are  $(q^2 + 1)q(q + 1)$  lines of  $\text{PG}(3, q)$  which are tangent to exactly one of the quadrics  $\mathcal{O}_0, \mathcal{O}_1, \dots, \mathcal{O}_q$ . Since the number of the lines of  $\text{PG}(3, q)$  not in  $\mathcal{S}$  is  $(q^2 + 1)q(q + 1)$ , this yields the lemma.  $\square$

We are now in the position to state the main theorem of this section, namely we provide a geometric construction of a starter set of  $\text{PG}(3, q)$ .

**Theorem 5.** *The lines tangent to  $\mathcal{O}$  through a fixed point  $P$  form a starter set of  $\text{PG}(3, q)$ .*

*Proof.* Let  $\alpha$  be the tangent plane to  $\mathcal{O}$  at  $P$  and denote by  $\{m_0, m_1, \dots, m_q\}$  be the  $q + 1$  tangents to  $\mathcal{O}$  at  $P$ . Assume that  $m_0$  belongs to  $\mathcal{S}$ .

If there is  $\delta \in S$  such that  $m_i^\delta = m_j$  with  $i, j \neq 0$ , then  $m_0^\delta \in \mathcal{S}$ , since  $\mathcal{S}$  is fixed by all the elements of  $S$ .

Suppose now that  $m_0^\delta \neq m_0$ . If it were  $\mathcal{O} = \mathcal{O}^\delta$ , then the line  $m_j$  would be incident with both  $P$  and  $P^\delta$ , both in  $\mathcal{O}$ ; hence,  $m_j$  could not be a tangent line. Thus,  $\mathcal{O} \neq \mathcal{O}^\delta$ .

This would mean that  $m_j$  is tangent to both  $\mathcal{O}$  and  $\mathcal{O}^\delta$  — a contradiction by Lemma 2. It follows that  $m_0^\delta = m_0$ . In particular, it follows from this argument that  $\delta$  is in  $S_1$ .

To conclude the proof, observe that if  $P^\delta \neq P$ , then  $m_j$  is tangent to  $\mathcal{O}^\delta$  at  $P^\delta$  and to  $\mathcal{O}$  at  $P$ . Then,  $\mathcal{O} = \mathcal{O}^\delta$  and  $\delta = \text{id}$ .  $\square$

## Thanks

The authors wish to express their gratitude to prof. G. Lunardon for several insightful discussions on the topics here-within investigated.

## References

- [1] E. F. Assmus, Jr. and J. D. Key, *Designs and their codes*, Cambridge Tracts in Mathematics, vol. 103, Cambridge University Press, Cambridge, 1992. MR MR1192126 (93j:51003)
- [2] Alexander Barg, Evgueni Krouk, and Henk C. A. van Tilborg, *On the complexity of minimum distance decoding of long linear codes*, IEEE Trans. Inform. Theory **45** (1999), no. 5, 1392–1405. MR MR1699066 (2000c:94016)
- [3] A. Barlotti and J. Cofman, *Finite Sperner spaces constructed from projective and affine spaces*, Abh. Math. Sem. Univ. Hamburg **40** (1974), 231–241.
- [4] L. M. Batten, *Combinatorics of finite geometries*, second ed., Cambridge University Press, Cambridge, 1997.
- [5] L. M. J. Bazzi and S. K. Mitter, *Encoding complexity versus minimum distance*, IEEE Trans. Inform. Theory **51** (2005), no. 6, 2103–2112. MR MR1699066 (2000c:94016)
- [6] T. Beth, D. Jungnickel, and H. Lenz, *Design theory. Vol. I*, second ed., Encyclopedia of Mathematics and its Applications, vol. 69, Cambridge University Press, Cambridge, 1999.
- [7] F. Bonetti and G. Lunardon, *Sugli  $S$ -spazi di traslazione*, Boll. Un. Mat. Ital. A (5) **14** (1977), no. 2, 368–374.
- [8] R. H. Bruck and R. C. Bose, *The construction of translation planes from projective spaces*, J. Algebra **1** (1964), 85–102.
- [9] R. G. Gallager, *Low-density parity-check codes*, IRE Trans. **IT-8** (1962), 21–28. MR MR0136009 (24 #B2048)
- [10] ———, *Low density parity-check codes*, M.I.T. Press, 1963.

- [11] J. W. P. Hirschfeld, *Finite projective spaces of three dimensions*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1985.
- [12] ———, *Projective geometries over finite fields*, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1998.
- [13] Y. Kou, S. Lin, and M. P. C. Fossorier, *Low-density parity-check codes based on finite geometries: a rediscovery and new results*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 2711–2736.
- [14] G. Lunardon, *Normal spreads*, Geom. Dedicata **75** (1999), no. 3, 245–261.
- [15] D. J. C. MacKay, *Good error-correcting codes based on very sparse matrices*, IEEE Trans. Inform. Theory **45** (1999), no. 2, 399–431.
- [16] Samuel J. MacMullan and Oliver M. Collins, *A comparison of known codes, random codes, and the best codes*, IEEE Trans. Inform. Theory **44** (1998), no. 7, 3009–3022. MR MR1672071 (99j:94082)
- [17] R. J. McEliece, *The theory of information and coding*, second ed., Encyclopedia of Mathematics and its Applications, vol. 86, Cambridge University Press, Cambridge, 2002. MR MR1899280 (2002k:94001)
- [18] T. J. Richardson and R. L. Urbanke, *Efficient encoding of low-density parity-check codes*, IEEE Trans. Inform. Theory **47** (2001), no. 2, 638–656.
- [19] B. Segre, *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane*, Ann. Mat. Pura Appl. (4) **64** (1964), 1–76.
- [20] H. Tang, J. Xu, Y. Kou, S. Lin, and K. Abdel-Ghaffar, *On algebraic construction of Gallager and circulant low-density parity-check codes*, IEEE Trans. Inform. Theory **50** (2004), no. 6, 1269–1279.